

Message Text

SECRET

PAGE 01 GENEVA 04326 212021Z
ACTION SS-25

INFO OCT-01 ISO-00 SSO-00 NSCE-00 DODE-00 CIAE-00
INRE-00 ACDE-00 DOEE-00 /026 W
-----074881 212030Z /50
O 211926Z MAR 78
FM USMISSION GENEVA
TO SECSTATE WASHDC IMMEDIATE 7476
INFO AMEMBASSY LONDON PRIORITY
AMEMBASSY MOSCOW PRIORITY

S E C R E T GENEVA 04326

EXDIS USCTB

PASS TO DOE

E.O. 11652: XGDS-3
TAGS: PARM US UK UR
SUBJECT: CTB NEGOTIATIONS: DESCRIPTION OF THE DATA
AUTHENTICATION SYSTEM

CTB MESSAGE NO. 181

FOLLOWING IS TEXT OF INFORMAL US DEL PAPER PROVIDING
INFORMATION ON DATA AUTHENTICATION WHICH WARNKE GAVE TO
SOVDEE AT MAR.20 HEADS OF DEL MEETING. BEGIN TEXT

DESCRIPTION OF THE DATA AUTHENTICATION SYSTEM

THE DATA AUTHENTICATION SYSTEM THAT THE UNITED STATES
IS SUGGESTING FOR USE IN INTERNAL STATIONS WOULD PROVIDE
A RELATIVELY SIMPLE METHOD FOR MAINTAINING THE OBJEC-
TIVITY OF THE DATA, ALLOW IMMEDIATE UNCODED ACCESS TO THE
DATA, AND ASSURE THE HOST COUNTRY THAT ONLY SEISMIC INFOR-
MATION IS OBTAINED FROM THE DATA. THIS SYSTEM, INSTALLED
IN EACH SEISMIC INSTALLATION, IS PART OF AN ELECTRONICS

SECRET

SECRET

PAGE 02 GENEVA 04326 212021Z

PACKAGE LOCATED NEAR THE SEISMOMETERS AT THE BOTTOM OF
A BOREHOLE. THE SYSTEM CONTAINS A STORED SET OF "KEY
WORDS" (ACTUALLY NUMBERS) USED IN THE AUTHENTICATION
PROCESS WHICH WOULD BE PROGRAMMED TO CHANGE AT APPROPRIATE
INTERVALS. THESE KEY WORDS WOULD BE STORED IN A
READ-ONLY MEMORY (I.E., THE NUMBERS IN THE MEMORY CANNOT
BE CHANGED) IN THE AUTHENTICATOR DOWNHOLE PACKAGE.

THE IMPORTANT FEATURES OF THIS DATA AUTHENTICATION SYSTEM ARE THE FOLLOWING:

1. AUTHENTICATION PROCESS

THE AUTHENTICATION PROCESS WOULD USE THE KEY WORDS IN CONJUNCTION WITH THE INPUT DATA TO GENERATE BY A MATHEMATICAL PROCEDURE AUTHENTICATION WORDS WHICH ARE INSERTED IN THE DATA STREAM AT APPROPRIATE POINTS. IF THE SEISMIC DATA WERE CHANGED IN ANY WAY THE AUTHENTICATION WORDS WOULD NO LONGER CORRESPOND TO THIS ALTERED SEISMIC DATA.

2. ACCESS TO THE SEISMIC DATA

THE SEISMIC DATA CAN BE READILY INTERPRETED AT ALL TIMES BY ALL TREATY PARTIES.

3. HOST COUNTRY ASSURANCE OF DATA INTEGRITY

ASSURANCE TO THE HOST COUNTRY THAT ONLY SEISMIC DATA IS BEING COLLECTED BY THE INSTALLATION CAN BE PROVIDED BY THE VERIFYING COUNTRY. AT AN APPROPRIATE TIME PRIOR TO THE INSTALLATION OF THE EQUIPMENT, THE DETAILED LOGIC OF THE AUTHENTICATOR PROCESS WILL BE EXPLAINED. AFTER THE
SECRET

SECRET

PAGE 03 GENEVA 04326 212021Z

KEY WORD HAS BEEN USED AND AUTOMATICALLY CHANGED (APPROXIMATELY TWO WEEKS), IT CAN BE SUPPLIED TO THE HOST COUNTRY. WITH THE AUTHENTICATOR LOGIC AND THE APPROPRIATE KEY WORD, THE DATA CAN BE SUBJECTED TO THE SAME LOGIC SEQUENCE APPLIED DURING THE DATA COLLECTION, AND THE RESULTING AUTHENTICATOR WORD COMPARED TO THE WORD APPENDED TO THE DATA. AGREEMENT BETWEEN THESE WORDS WILL PROVIDE THE DESIRED ASSURANCE TO BOTH PARTIES. END TEXT. WARNKE

SECRET

NNN

Message Attributes

Automatic Decaptioning: Z
Capture Date: 01 jan 1994
Channel Indicators: n/a
Current Classification: UNCLASSIFIED
Concepts: DATA, SEISMOLOGY, NEGOTIATIONS, AUTHENTICATIONS, COMMUNICATION LINES
Control Number: n/a
Copy: SINGLE
Draft Date: 21 mar 1978
Decaption Date: 20 Mar 2014
Decaption Note: 25 YEAR REVIEW
Disposition Action: RELEASED
Disposition Approved on Date:
Disposition Case Number: n/a
Disposition Comment: 25 YEAR REVIEW
Disposition Date: 20 Mar 2014
Disposition Event:
Disposition History: n/a
Disposition Reason:
Disposition Remarks:
Document Number: 1978GENEVA04326
Document Source: CORE
Document Unique ID: 00
Drafter: n/a
Enclosure: n/a
Executive Order: X3
Errors: N/A
Expiration:
Film Number: D780124-1052
Format: TEL
From: GENEVA
Handling Restrictions:
Image Path:
ISecure: 1
Legacy Key: link1978/newtext/t19780344/aaaabkse.tel
Line Count: 102
Litigation Code IDs:
Litigation Codes:
Litigation History:
Locator: TEXT ON-LINE, ON MICROFILM
Message ID: 3ed860c3-c288-dd11-92da-001cc4696bcc
Office: ACTION SS
Original Classification: SECRET
Original Handling Restrictions: ONLY
Original Previous Classification: n/a
Original Previous Handling Restrictions: n/a
Page Count: 2
Previous Channel Indicators: n/a
Previous Classification: SECRET
Previous Handling Restrictions: ONLY
Reference: n/a
Retention: 0
Review Action: RELEASED, APPROVED
Review Content Flags:
Review Date: 15 jun 2005
Review Event:
Review Exemptions: n/a
Review Media Identifier:
Review Release Date: n/a
Review Release Event: n/a
Review Transfer Date:
Review Withdrawn Fields: n/a
SAS ID: 3259477
Secure: OPEN
Status: NATIVE
Subject: CTB NEGOTIATIONS: DESCRIPTION OF THE DATA AUTHENTICATION SYSTEM CTB MESSAGE NO. 181
TAGS: PARM, US, UK, UR
To: STATE
Type: TE
vdkgvwkey: odb://SAS/SAS.dbo.SAS_Docs/3ed860c3-c288-dd11-92da-001cc4696bcc
Review Markings:
Sheryl P. Walter
Declassified/Released
US Department of State
EO Systematic Review
20 Mar 2014
Markings: Sheryl P. Walter Declassified/Released US Department of State EO Systematic Review 20 Mar 2014